UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/751,899	12/27/2000	David W. Grawrock	42390P9844	9094

8791 7590 12/01/2003

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD, SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
MAHMOUDI, HASSAN	
ART UNIT	**PAPER NUMBER**
2175	3

DATE MAILED: 12/01/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/751,899	Applicant(s) GRAWROCK, DAVID W.
	Examiner Tony Mahmoudi	Art Unit 2175

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s) _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in
> (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or
> (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 12-21 are rejected under 35 U.S.C. 102(e) as being anticipated by England (U.S. Patent No. 6,330,670.)

As to claim 12, England teaches an integrated circuit device (see column 5, lines 52-62) comprising:

a boot block memory unit (see column 11, lines 26-47, and see figures 7A-7C); and

a trusted platform module communicatively coupled to the boot block memory unit (see column 11, lines 48-53), the trusted platform module to produce a combination key by combining a first incoming keying material with a second keying material internally stored within the integrated circuit (see column 7, line 51 through column 8, line 6, and see column 13, lines 60-67) and to decrypt a second BIOS area to recover a second segment of BIOS code (see column 7, lines 45-62.)

As to claim 13, England teaches wherein the boot block memory unit to load a BIOS code including a first BIOS area and a second BIOS area (see column 11, lines 30-63), the first BIOS area being an encrypted first segment of the BIOS code and the second BIOS area being an encrypted second segment of the BIOS code (see column 10, lines 4-13, and see column 16, lines 52-66.)

As to claim 14, England teaches wherein the trusted platform module to decrypt the first BIOS area to recover the first segment of the BIOS code (see column 10, lines 41-51.)

As to claim 15, England teaches a platform (see column 52-62) comprising:

an input/output control hub (ICH) (see column 6, lines 9-23);

a non-volatile memory unit coupled to the ICH, the non-volatile memory unit including a BIOS code including a first BIOS area and a second BIOS area (see figure 1A), the first BIOS area being an encrypted first segment of the BIOS code and the second BIOS area being an encrypted second segment of the BIOS code (see column 10, lines 4-13, and see column 16, lines 52-66);

For the remaining steps of this claim, the applicant is kindly directed to remarks and discussions made in claim 12 above.

As to claim 16, England teaches wherein the trusted platform module to further decrypt the first BIOS area to recover the first segment of the BIOS code in an non-encrypted format (see column 10, lines 41-51.)

As to claim 17, England teaches the platform further comprising a hard disk drive coupled to the ICH (see figure 1A.)

As to claims 18 and 21, England teaches wherein the trusted platform module to further unbind keying material associated with the hard disk drive to access contents stored within the hard disk drive (see figure 1B.)

As to claim 19, England teaches a program loaded into readable memory for execution by a trusted platform module of a platform (see column 5, lines 39-51.) For the remaining steps of this claim, the applicant is kindly directed to remarks and discussions made in claims 12 and 15 above.

As to claim 20, England teaches wherein the first BIOS area is the first segment of the BIOS code encrypted with a keying material (see column 10, lines 4-13, and see column 16, lines 52-66) and the second BIOS area is the second segment of the BIOS code encrypted with the combination key (see column 7, line 51 through column 8, line 6, and see column 13, lines 60-67.)

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-5 and 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over England (U.S. Patent No. 6,330,670) in view of Reardon (U.S. Patent No. 6,212,635.)

As to claim 1, England teaches a method (see Abstract) comprising:

authenticating a user of a platform during a Basic Input/Output System (BIOS) boot process (see column 6, lines 9-23, and see column 7, lines 33-50);

combining the first keying material with a second keying material internally stored within the platform in order to produce a combination key (see column 7, line 51 through column 8, line 6, and see column 13, lines 60-67); and

using the combination key to decrypt a second BIOS area to recover a second segment of BIOS code (see column 7, lines 45-62.)

England does not teach: releasing a first keying material from a token communicatively coupled to the platform in response to authenticating the user.

Reardon teaches a network security system (see Abstract), in which he teaches releasing a first keying material from a token communicatively coupled to the platform in response to authenticating the user (see column 3, lines 18-67, and see column 8, lines 43-67.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified England to include releasing a first keying material from a token communicatively coupled to the platform in response to authenticating the user.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified England but the teaching of Reardon, because releasing a first keying material from a token communicatively coupled to the platform in response to authenticating the user, would enhance the system security, because the token could be easily transported, like an ID card. The "key" to the data can therefore be stored away from the Data, as taught by Reardon (see column 2, lines 51-67.)

As to claim 2, England as modified teaches the method further comprising: continuing the BIOS boot process (see England, column 11, lines 54-63.)

As to claim 3, England as modified teaches wherein prior to authenticating the user (see England, column 6, lines 9-23, and see column 7, lines 33-50), the method comprises:

loading a BIOS code including a first BIOS area and a second BIOS area (see England, column 11, lines 30-63), the first BIOS area being an encrypted first segment of the BIOS code and the second BIOS area being an encrypted second segment of the BIOS code (see England, column 10, lines 4-13, and see column 16, lines 52-66.)

As to claim 4, England as modified teaches wherein after loading of the BIOS code, the method further comprises:

decrypting the first BIOS area to recover the first segment of the BIOS code (see England, column 10, lines 41-51.)

As to claim 5, England as modified teaches the method further comprising:

unbinding keying material associated with a non-volatile storage device to access contents stored within the non-volatile storage device (see England, figure 1B.)

As to claim 8, England as modified teaches wherein the second keying material is stored within internal memory of a trusted platform module (see England, Abstract; see column 15, lines 62-67, and column 16, lines 42-49.)

As to claim 9, England as modified teaches wherein the second keying material is stored within a section of access-controlled system memory of the platform (see England, column 19, lines 18-28, and see figure 10.)

As to claim 10, England as modified teaches wherein prior to authenticating the user, the method comprises:

loading a BIOS code including a first BIOS area (see England, column 11, lines 30-63) being a first segment of the BIOS code encrypted using a selected keying material (see England, column 10, lines 4-13, and see column 16, lines 52-66); and

loading an integrity metric including a hash value of an identification information of the platform (see England, column 2, line 60 through column 3, line 30.)

As to claim 11, England as modified teaches wherein the identification information includes a serial number of an integrated circuit device employed within the platform (see England, column 18, lines 47-54.)

5. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over England (U.S. Patent No. 6,330,670) in view of Reardon (U.S. Patent No. 6,212,635), as applied to claims 1-5 above, and further in view of Adams et al (U.S. Patent No. 6,363,485.)

As to claim 6, England as modified still does not teach wherein the combination key is a value formed by performing an exclusive OR operation on both the first keying material and the second keying material.

Adams et al teaches a multi-factor biometric authenticating device and method (see Abstract), in which he teaches wherein the combination key is a value formed by performing an exclusive OR operation on both the first keying material and the second keying material (see Abstract, and see column 3, line 59 through column 4, line 3.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified England as modified, to include wherein the combination key is a value formed by performing an exclusive OR operation on both the first keying material and the second keying material.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified England as modified, by the teaching of Adams et al, because wherein the combination key is a value formed by performing an exclusive OR operation on both the first keying material and the second keying material, would provide an effective way of combining keys in encryption and authentication environment.

As to claim 7, England as modified teaches wherein authentication of the user is performed through biometrics (see Adams et al, Abstract, and see column 2, lines 31-47.)

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The following patents are cited to further show the state of art with respect to methods and systems of secured boot program and user authentications in general:

Patent/Pub. No.	Issued to	Cited for teaching
US 5,007,082	Cummins	Computer software encryption apparatus.
US 6,061,794	Angelo et al.	Secured device communications and bus architecture.
US 6,463,537	Tello	Modified BIOS and computer Motherboard security.
US 2003/0018892	Tello	Modified BIOS and secured booting of a computer.

7. Any inquiries concerning this communication or earlier communications from the examiner should be directed to Tony Mahmoudi whose telephone number is (703) 305-4887. The examiner can normally be reached on Mondays-Fridays from 08:00 am to 04:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici, can be reached at (703) 305-3830.

tm

November 12, 2003

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100